UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/911,511	07/25/2001	Masashi Mitomo	1341.1102	4245

21171 7590 11/12/2004

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER
TAYLOR, NICHOLAS R

ART UNIT	PAPER NUMBER
2141	

DATE MAILED: 11/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/911,511	Applicant(s) MITOMO ET AL.	
	Examiner Nicholas R Taylor	Art Unit 2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 07/25/01.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-21 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-21 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 25 July 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 have been examined and are rejected.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-4, 7-11, 14-18, and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Carter et al. (US PGPub 2001/0039579 A1.)

5. As per claims 1, 8, and 15, Carter teaches a system interposed between a client and a server (Carter, Fig. 1, specifically item 18), said server providing services depending on access requests from said client, for passing to said server only a correct

access request from said client, said filtering device comprising: (Carter, page 51, paragraph 1050)

an incorrect pattern database which stores patterns of incorrect accesses to said server; (Carter, page 51, paragraph 1056, specifically the Attacks Sequence Database)

an estimation unit which estimates the correctness of the access request on the basis of the patterns of incorrect accesses stored in said incorrect pattern database and a predetermined estimation rule; (Carter, page 51, paragraphs 1050-1056)

and a decision unit which decides, on the basis of a result of estimation by said estimation unit and a predetermined decision rule, whether the access request is to be passed to said server (Carter, page 51, paragraphs 1050-1056, specifically the Intrusion Analysis Algorithm.)

6. As per claims 2, 9, and 16, Carter teaches a system wherein said estimation unit estimates that the access request is an incorrect access when the access request corresponds to any one of the patterns of incorrect accesses stored in said incorrect pattern database, (Carter, page 51, paragraph 1056, specifically the Attack Sequence Database) and estimates that the access request is a correct access when the access request does not correspond to any one the patterns of incorrect accesses stored in the incorrect pattern database, and (Carter, page 51, paragraphs 1050-1056, specifically the Neural Network Inference Engine Algorithm)

said decision unit decides that the access request which is estimated as an incorrect access by said estimation unit is not to be passed to said server, and decides that the access request which is estimated as a correct access by said estimation unit is to be passed to said server (Carter, page 51, paragraph 1050.)

7. As per claims 3, 10, and 17, Carter teaches a system wherein said estimation unit calculates a predetermined estimation value depending on the degree of correspondence between the access request and the patterns of incorrect accesses stored in said incorrect pattern database, and (Carter, page 51, paragraph 1050 and 1062-1065, and also page 52, paragraphs 1070-1090, specifically the Event Learning Algorithm Markov Model for probability)

said decision unit compares the estimation value calculated by said estimation unit with a predetermined threshold value to decide whether the access request is to be passed to said server (Carter, page 51, paragraph 1050 and 1062-1065, and also page 52, paragraphs 1070-1090, specifically the Event Learning Algorithm Markov Model for probability.)

8. As per claims 4, 11, and 18, Carter teaches a system further comprising:

a correct pattern database which stores patterns of correct accesses to said server; and (Carter, page 49, paragraph 0997-0998, specifically the Security Reference Database)

an advance decision unit which decides whether the access request corresponds to any one of the patterns of correct accesses stored in said correct pattern database prior to estimation of correctness performed by said estimation unit, (Carter, page 49, paragraph 0997 to page 50, paragraph 1015, specifically the Security Reference Monitor checking to see if a user has made a correct access)

wherein said estimation unit estimates correctness of only that access request which said advance decision unit decides that does not correspond to the patterns of correct accesses stored in said correct pattern database (Carter, page 51, paragraph 1050-1055, specifically the Intrusion Analysis Algorithm.)

9. As per claims 7, 14, and 21, Carter teaches a system further comprising an updating unit which updates the incorrect pattern database, the correct pattern database, the estimation rule, the decision rule, the external transmission rule, the storage rule, or an updating rule on the basis of a predetermined updating rule (Carter, page 51, paragraphs 1050-1055, specifically when the Intrusion Analysis Algorithm updates by collecting new strings of network intrusion detection signatures.)

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claim 5, 6, 11, 12, 19, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carter et al. (US PGPub 2001/0039579 A1) and Trcka et al. (US PGPub 2001/0039579 A1.)

12. As per claims 5, 12, and 19, Carter teaches the system above. However, Carter fails to teach the system further comprising an external transmission unit which transmits an access request which is decided not to be passed to said server by said decision unit to a predetermined external device on the basis of a predetermined external transmission rule.

Trcka teaches a network security and surveillance system that records rejected access transactions to an external device (Trcka, page 10, paragraph 0105 to page 11, paragraph 0107, specifically the Good-Data Cyclic Recorders, see also Fig 8.)

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to have combined Carter and Trcka to provide an external transmission unit which transmits an access request which is decided not to be passed to a server by a decision unit to a predetermined external device on the basis of a predetermined external transmission rule in the said system of Carter, because doing so would allow recordings that can be used to detect and analyze break-ins and other network anomalies. This is stated as referenced in the art (Trcka, page 2, paragraph 0013.)

13. As per claims 6, 13, and 20, Carter teaches the system above. However, Carter fails to teach the system further comprising a storage unit which stores an access request which is decided not to be passed to said server by said decision unit on the basis of a predetermined storage rule.

Trcka teaches a network security and surveillance system that records rejected access transactions to a storage device (Trcka, page 10, paragraph 0105 to page 11, paragraph 0107, specifically the Good-Data Cyclic Recorders, see also Fig 8.)

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to have combined Carter and Trcka to provide a storage unit which stores an access request which is decided not to be passed to a server by a decision unit on the basis of a predetermined storage rule in the said system of Carter, because doing so would allow recordings that can be used to detect and analyze break-ins and other network anomalies. This is stated as referenced in the art (Trcka, page 2, paragraph 0013.)

Conclusion

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nicholas R Taylor whose telephone number is (571) 272-3889. The examiner can normally be reached on Monday-Friday, 8:00am to 5:30pm, with alternating Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is (703) 305-3718.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nicholas Taylor
Assistant Examiner
Art Unit 2141

LE HIEN LUU
PRIMARY EXAMINER